4N

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/637,229	08/11/2000	Cetin K. Koc	245-55512	7362

7590 03/08/2005

Klarquist Sparkman Campbell
Leigh & Whinston LLP
One World Trade Center Suite 1600
121 S W Salmon Street
Portland, OR 97204

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/637,229	KOC ET AL.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 July 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 August 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment filed on 02 July 2004 has been noted and made of record.

2. Claims 1-21 have been presented for examination.

Response to Arguments

3. In response to applicant's argument that a field representation select input to clarify that the field select input previously recited is associated with selection of a particular field type such as a prime field GF(p) or a binary extension field GF(2^k), a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim. In a claim drawn to a process of making, the intended use must result in a manipulative difference as compared to the prior art. See *In re Casey*, 370 F.2d 576, 152 USPQ 235 (CCPA 1967) and *In re Otto*, 312 F.2d 937, 939, 136 USPQ 458, 459 (CCPA 1963).

4. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features, such as the field select input previously recited being associated with the selection of a particular field type such as a prime field GF(p) or a binary extension field GF(2^k), upon which applicant relies are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

5. In regards to Applicant's argument that the claims cannot be rejected under 102(e) since CypherCalc is not a patent, the Examiner agrees and can only assume that the previous Examiner made a mistake and meant to reject the claims under 102(a).

6. As per the Applicant's argument that the disclosed date of the disclosed version of CypherCalc is plainly wrong, the Examiner disagrees. After a brief search for http://www.cyphercalc.com at http://www.archive.org, the Examiner discovered a very similar disclosure of CypherCalc dated 08 October 1999.

7. Therefore, the rejection of the claims under CypherCalc is upheld as being proper.

8. See further rejections that follow.

Claim Rejections - 35 USC § 101

9. As per claims 1-5, merely claimed as a computer program representing a computer listing *per se*, that is, descriptions or expressions of such a program and that is, descriptive material *per se*, non-functional descriptive material, and is not statutory because it is not a physical "thing" nor a statutory process, as there are not "acts" being performed. Such claimed computer programs do not define any structural and functional interrelationships between the computer program and other claimed aspects of the invention which permit the computer program's functionality to be realized. Since a computer program is merely a set of instructions capable of being executed by a computer, the program itself is not a process, without the computer-readable medium needed to realize the computer program's functionality. In contrast, a claimed computer-readable medium encoded with a computer program defines structural and functional interrelationships between the computer program and the medium which permit the computer program's functionality to be realized, and is thus statutory. **Warmerdam**, 33 F.3d at 1361, 31

USPQ2d at 1760. **In re Sarkar**, 588 F.2d 1330, 1333, 200 USPQ 132, 137 (CCPA 1978). See MPEP § 2106(IV)(B)(1)(a). Wherein the Examiner has interpreted the term module in accordance with the first definition provided by **Microsoft Computer Dictionary, 5th Edition**, which reads:

> In programming, a collection of routines and data structures that performs a particular task or implements a particular abstract data type. Modules usually consist of two parts: an interface, which lists the constants, data types, variables, and routines that can be accessed by other modules or routines; and an implementation, which is private and which contains the source code that actually implements the routines in the module.

Claim Rejections - 35 USC § 112

10. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

11. Claims 1-21 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Examiner would like to point out that where applicant acts as his or her own lexicographer to specifically define a term of a claim contrary to its ordinary meaning, the written description must clearly redefine the claim term and set forth the uncommon definition so as to put one reasonably skilled in the art on notice that the applicant intended to so redefine that claim term. *Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1357, 52 USPQ2d 1029, 1033 (Fed. Cir. 1999). The term "field-representation-select input" repeated through many of the claims is not clearly defined. The Applicant fails to meet the requirements of defining a term as set forth in the MPEP § 2106. In order to define/redefine a term, the Applicant must do so "with reasonable clarity, deliberateness, and precision" and must " set out his uncommon definition in some manner within the patent disclosure' so as to give one of ordinary skill in the

art notice of the change" in meaning. The Applicant fails to clearly, deliberately and precisely define the term field-representation-select input. Furthermore, the Applicant fails to set out the uncommon definition in the instant application's disclosure.

12. The term "GF(p)" in claims 8-11 is a relative term which renders the claim indefinite. The term "GF(p)" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

13. The term "$GF(2^m)$" in claims 8-11 is a relative term which renders the claim indefinite. The term " $GF(2^m)$" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

14. The term "m" in claim 11 is a relative term which renders the claim indefinite. The term "m" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

15. The term "e" in claim 11 is a relative term which renders the claim indefinite. The term "e" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

16. The term "w" in claim 11 is a relative term which renders the claim indefinite. The term "w " is not defined by the claim, the specification does not provide a standard for ascertaining the

requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

17. Claim 18 provides for the use of a computer readable medium executing instructions, but, since the claim does not set forth any steps involved in the method/process, it is unclear what method/process applicant is intending to encompass. A claim is indefinite where it merely recites a use without any active, positive steps delimiting how this use is actually practiced.

18. Claim 18 is rejected under 35 U.S.C. 101 because the claimed recitation of a use, without setting forth any steps involved in the process, results in an improper definition of a process, i.e., results in a claim which is not a proper process claim under 35 U.S.C. 101. See for example *Ex parte Dunki*, 153 USPQ 678 (Bd.App. 1967) and *Clinical Products, Ltd.* v. *Brenner*, 255 F. Supp. 131, 149 USPQ 475 (D.D.C. 1966).

Claim Rejections

19. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

20. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

21. Claims 1-5, 12-15, and 19-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,745,98 to Monier, hereinafter Monier, in view of U.S. Patent No. 6,397,241 to Glaser et al., hereinafter Glaser.

22. As per claim 1, Monier discloses a multiplication module, comprising:

a first input and a second input configured to receive a first operand and a second operand, respectively, represented as elements of a finite field (column 3, lines 38-45, column 5, lines 55-60, i.e. "multiplicand A and multiplier B");

an output configured to deliver a Montgomery product of the first operand and the second operand (column 3, lines 38-45, column 7, lines 55-59, i.e. "a method for implementation of modular multiplication according to the Montgomery method").

23. Monier does not disclose a field- representation-select input configured to select multiplication of the first and second operands based on a selected finite field representation.

24. Glaser teaches a field- representation-select input configured to select multiplication of the first and second operands based on a selected finite field representation (column 2, lines 39-46, column 13, line 65 to column 14, line 32).

25. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a field- representation-select input configured to select multiplication of the first and second operands based on a selected finite field representation, since Glaser states at column 1, lines 30-35 that such a modification would achieve high performance, low cost, and low-power while being able to compute several different encryption algorithms.

26. Regarding claim 2, Glaser discloses wherein the field select input is configurable to select a prime field representation or a binary extension field representation (column 2, lines 39-46, column 13, line 65 to column 14, line 32).

27. With regards to claims 3 and 4, Monier teaches wherein the first operand is processed bit-wise and the second operand is processed word-wise (column 6, line 62 to column 7, line 46, column 9, lines 7-46).

28. Regarding claims 5, 9, 10, 13, 17, and 20, Monier discloses a dual-field adder that is configurable to execute addition without carry, based on a value supplied to the field select input (column 7, lines 19-23, column 10, lines 46-50).

29. As per claim 12, Monier discloses a dual-field adder, comprising:

a first input and a second input situated to receive respective operands (column 3, lines 38-45, column 5, lines 55-60, i.e. "multiplicand A and multiplier B");

an addition module, configured to add values supplied to the first and second input according to a value supplied to the field-representation-select input (column 7, lines 19-23, column 10, lines 46-50).

30. Monier does not disclose a field-representation-select input.

31. Glaser teaches a field- representation-select input (column 2, lines 39-46, column 13, line 65 to column 14, line 32).

32. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a field- representation-select input configured to select multiplication of the first and second operands based on a selected finite field representation, since Glaser states at column 1, lines 30-35 that such a modification would achieve high performance, low cost, and low-power while being able to compute several different encryption algorithms.

33. With regards to claims 14 and 15, Monier discloses wherein the addition module includes an exclusive OR gate situated and configured to receive a bit of the first operand and a bit of the second operand (Figure 1 [blocks 30, 31]).

34. As per claim 19, Monier discloses a Montgomery multiplier configured to determine a Montgomery product of a first operand and a second operand, the multiplier comprising:

an output that delivers the Montgomery product (column 3, lines 38-45, column 7, lines 55-59).

35. Monier does not disclose a field-select input for selection of arithmetic operations corresponding to a prime field or a binary extension field.

36. Glaser teaches a field-select input for selection of arithmetic operations corresponding to a prime field or a binary extension field (column 2, lines 39-46, column 13, line 65 to column 14, line 32).

37. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a field- representation-select input configured to select multiplication of the first and second operands based on a selected finite field representation, since Glaser states at column 1, lines 30-35 that such a modification would achieve high performance, low cost, and low-power while being able to compute several different encryption algorithms.

38. With regards to claim 21, Monier discloses a scalable Montgomery multiplication module situated and configured to obtain a Montgomery product of the first operand and the second operand (column 3, lines 38-45, column 7, lines 55-59).

39. Claims 6, 7, and 16-18 are rejected under 35 U.S.C. 102(b) as being anticipated by Monier.

40. As per claim 6, Monier discloses a cryptographic processor, comprising:

inputs for receiving a first and a second cryptographic parameter represented as elements of a finite field (column 3, lines 38-45, column 5, lines 55-60, i.e. "multiplicand A and multiplier B"); and

a multiplication module configured to receive the cryptographic parameters from the inputs, the multiplication module including at least two processing units configured to determine a Montgomery product of the cryptographic parameters, each processing unit receiving a bit corresponding to the first parameter and partial words of the second parameter (Figure 1 [blocks 19, 20], column 3, lines 38-45, column 5, lines 27-37, column 7, lines 55-59).

41. Regarding claim 7, Monier discloses wherein at least one processing unit is configured to communicate intermediate values of partial words of the Montgomery product to a different processing unit (column 6, line 62 to column 7, line 46, column 9, lines 7-46).

42. As per claim 16, Monier discloses a method of determining a Montgomery product of a first cryptographic parameter and a second cryptographic parameter, the method comprising:

representing the first cryptographic parameter as a series of bits (column 3, lines 38-45, column 5, lines 55-60);

representing the second cryptographic parameter as a series of words (column 3, lines 38-45, column 5, lines 55-60);

determining an intermediate value of a contribution to the Montgomery product based on a first bit of the first cryptographic parameter and the words of the second cryptographic parameter in a first pipeline stage (column 6, line 62 to column 7, line 46, column 9, lines 7-46);

determining intermediate values of contributions to the Montgomery product based on remaining bits of the first cryptographic parameter in respective pipeline stages that receive the words of the second cryptographic parameter and an intermediate value from a prior pipeline stage (column 6, line 62 to column 7, line 46, column 9, lines 7-46); and

combining the intermediate values to form the Montgomery product of the first cryptographic parameter and the second cryptographic parameter (column 3, lines 38-45, column 7, lines 55-59).

43. With regards to claim 18, Monier discloses a computer-readable medium containing instructions for executing the method of claim 17 (Figure 1 [block 35]).

44. Claims 8-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Monier in view of Glaser OR Applicant's Admitted Prior Art, hereinafter AAPA.

45. Regarding claim 8, Monier does not teach a field-representation-select input in communication with the multiplication module for selection of an arithmetic operation in the multiplication module to be performed in accordance with $GF(p)$ or $GF(2^m)$ arithmetic.

46. Glaser discloses a field-representation-select input in communication with the multiplication module for selection of an arithmetic operation in the multiplication module to be performed in accordance with $GF(p)$ or $GF(2^m)$ arithmetic (column 2, lines 39-46, column 13, line 65 to column 14, line 32).

47. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a field- representation-select input configured to select multiplication of the first and second operands based on a selected finite field representation, since Glaser states at column 1, lines 30-35 that such a modification would achieve high performance, low cost, and low-power while being able to compute several different encryption algorithms.

48. AAPA discloses using $GF(2^m)$ and GF(p) on page 2 of the specification.

49. It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement $GF(2^m)$, since AAPA discloses that there are efficient software implementations of such arithmetic, especially if an irreducible polynomial generating the finite field is chosen arbitrarily.

50. It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement GF(p), since AAPA discloses that there are scalable Montgomery multiplier designs for this particular finite field.

51. Concerning claim 11, Monier teaches wherein the first and second cryptographic parameters are represented as $_m$ bits and $_e$ words of word length, wherein [(m + 1) / w] (column 4, lines 1-47).

52. Claims 1, 6, and 12 are rejected under 35 U.S.C. 102(a) as being anticipated by EPS/Solutions, herein EPS (Cyphercalc The Cryptographer's Calculator).

53. As per claim 1, EPS teaches a multiplication module, comprising: a first input and a second input configured to receive a first operand and a second operand, respectively, represented as elements of a finite field', an output configured to deliver a Montgomery product of the first operand and the second operand, and a field-select input configured to select multiplication of the first and second operands based on a selected finite field (refer to Montgomery Image and Product calculators). Wherein the field representation select input is drawn to the figure on page 4 of 6, detailing converting to Hex or Decimal.

54. As per claim 6, EPS teaches A cryptographic processor, comprising: inputs for receiving a first and a second cryptographic parameter represented as elements of a finite field; and a multiplication module configured to receive the cryptographic parameters from the inputs, the multiplication module including processing units configured to determine a Montgomery product of the cryptographic parameters, each processing unit receiving a bit corresponding to the first parameter and partial words of the second parameter (refer to Montgomery Image and Product calculators). Wherein the field representation select input is drawn to the figure on page 4 of 6, detailing converting to Hex or Decimal.

55. As per claim 12, EPS teaches a dual-field adder, comprising: a first input and a second input situated to receive respective operands', a field-select input; and an addition module, configured to add values supplied to the first and second input according to a value supplied to the field select input (see Description). Wherein the field representation select input is drawn to the figure on page 4 of 6, detailing converting to Hex or Decimal.

56. Claims 2, 3, 4, 8, 9, 10, 11 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over EPS in view of Brandstrom (USP 4,322,577).

57. As per claims 2 and 19, EPS teaches his system is for the use of performing calculation based on cryptographical algorithms (refer to Description). EPS teaches the choice of determining which field to compute Montgomery products (see Montgomery Product). EPS fails to explicitly disclose the use of prime fields and binary extension fields. Brandstrom teaches a cryptographical system in which prime fields and binary extension fields are used to carry out the Montgomery multiplications (column 4, lines 40-55 and column 5, lines 20-25). Binary fields and primary fields are well suited to a computer's architecture and cryptographic fundamental security.

58. In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Brandstrom within the system of EPS because EPS'S program allows the user to enter the finite field and Brandstrom teaches finite fields for use on a computer.

59. As per claim 3, EPS teaches the first operand is processed bit-wise and the second operand is processed word-wise (see Montgomery product).

60. As per claim 4, EPS teaches the second operand is divided into multiple words that are multiplied with bits of the first operand (see Montgomery product).

61. As per claim 8, the examiner recites the same rationale for the motivation as recited in the rejection of claim 2 to incorporate the teachings of Brandstrom within the system of EPS.

62. As per claim 9, EPS teaches the arithmetic operation selectable with the field select input is field addition (see Description).

63. As per claim 10, EPS teaches a dual-field adder in communication with the field-select input (see Description).

64. As per claim 11, EPS teaches the first and second cryptographic parameters are represented as m bits and e words of word length (see Montgomery Products).

65. Claims 5, 13, 14, and 15 are rejected under 35 U.S.C. 1O3(a) as being unpatentable over EPS in view of Iwamura et al, herein Iwamura, (USP 5,321 ,752).

66. As per claims 5 and 13, EPS teaches a dual-field adder that is configurable (see

Description). The user supplies the modulus to the arithmetic functions. EPS does not disclose that the addition is executed without carry. Iwamura teaches that in the Galois field, there is no carry bit, which simplifies the hardware (column 18, lines 3-6).

67. Therefore, it would be advantageous to not use a carry bit when operating in the Galois field. In view of this, it would have been obvious to one of ordinary skill in the ad at the time the invention was made to employ the teaching of Iwamura within the system of EPS because it would minimize the hardware requirements.

68. As per claim 14, EPS teaches the addition module includes an exclusive OR gate situated and configured to receive a bit of the first operand and a bit of the second operand (see Description).

69. As per claim 15, EPS teaches the addition module includes a first and a second exclusive OR gates situated and configured to receive a bit of the first operand and a bit of the second operand, respectively (see Description).

70. Claims 7 and 16, are rejected under 35 U.S.C. 103(a) as being unpatentable over EPS in view of Monier (USP 5,745,398).

71. As per claim 7, EPS fails to teach at least one processing unit is configured to communicate intermediate values of partial words of the Montgomery product to a different processing unit. Monier teaches at least one processing unit is configured to communicate

intermediate values of partial words of the Montgomery product to a different processing unit as a way of pipelining to increase the performance of the system (column 3, lines 38-67).

72. It would be advantageous to use parallel processing in order to decrease the overall computation time required to execute a calculation. In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Monier within the system of EPS because it would decrease the total time needed to solve complication computations.

73. As per claim 16, EPS teaches a method of determining a Montgomery product of a first cryptographic parameter and a second cryptographic parameter, the method comprising: representing the first cryptographic parameter as a series of bits and representing the second cryptographic parameter as a series of words (see Montgomery Images and Montgomery Products). EPS fails to teach determining an intermediate value of a contribution to the Montgomery product based on a first bit of the first cryptographic parameter and the words of the second cryptographic parameter in a first pipeline stage; and determining intermediate values of contributions to the Montgomery product based on remaining bits of the first cryptographic parameter in respective pipeline stages that receive the words of the second cryptographic parameter and an intermediate value from a prior pipeline stage. Monier teaches determining an intermediate value of a contribution to the Montgomery product based on a first bit of the first cryptographic parameter and the words of the second cryptographic parameter in a first pipeline stage, and determining intermediate values of contributions to the Montgomery product based on remaining bits of the first cryptographic parameter in respective pipeline stages that receive the

words of the second cryptographic parameter and an intermediate value from a prior pipeline stage (column 3, lines 38-67).

74. Monier teaches at least one processing unit is configured to communicate intermediate values of partial words of the Montgomery product to a different processing unit as a way of pipelining to increase the performance of the system.

75. It would be advantageous to use parallel processing in order to decrease the overall computation time required to execute a calculation. In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Monier within the system of EPS because it would decrease the total time needed to solve complication computations.

76. Claims 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over EPS and Monier as applied to claim 16 above, and further in view of Iwamura.

77. As per claim 17, examiner recites the same rationale for the motivations as recited in the rejection of claims 5 and 13 to incorporate the teachings of Iwamura within the combined system of EPS and Monier.

78. As per claim 18, EPS teaches a computer-readable medium containing instructions for executing the method of claim 17 (see Description).

79. Claims 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over EPS and Brandstrom as applied to claim 19 above, and further in view of Iwamura.

80. As per claim 20, examiner recites the same rationale for the motivations as recited in the rejection of claims 5 and 13 to incorporate the teachings of Iwamura within the combined system of EPS and Brandstrom.

81. As per claim 21, EPS teaches a scalable Montgomery multiplication module situated and configured to obtain a Montgomery product of the first operand and the second operand (see Montgomery Product and Montgomery Image).

Conclusion

82. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

83. The following patents are cited to further show the state of the art with respect to Montgomery multiplication techniques, such as:

United States Patent No. 6,252,959 to Paar et al., which is cited to show a method to reduce the number of inverses in the underlying field GF(2^m).

United States Patent No. 6,356,636 to Foster et al., which is cited to show fast modular multiplication.

United States Patent Application Publication No. 2002/0013799 to Blaker, which is cited to show accelerated Montgomery multiplication using plural multipliers.

United States Patent Application Publication No. 2002/0039418 to Dror et al., which is cited to show an extension of serial/parallel Montgomery modular multiplication in both the prim number field and the polynomial based number field.

United States Patent Application Publication No. 2005/0041811 to Kobayashi et al., which is cited to show modular inversion for information security.

84. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

85. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

86. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131

clf

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100